Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications

Journal Item

How to cite:

Bottarelli, Mirko; Karadimas, Petros; Epiphaniou, Gregory; Kbaier, Dhouha and Maple, Carsten (2021). Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications. IEEE Transactions on Vehicular Technology, 70(3) pp. 2310–2321.

Link(s) to article on publisher's website:
http://dx.doi.org/doi:10.1109/TVT.2021.3056638

Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications

Mirko Bottarelli, *Student Member, IEEE,* Petros Karadimas, *Senior Member, IEEE,* Gregory Epiphaniou, *Member, IEEE,* Dhouha Kbaier Ben Ismail, *Member, IEEE,* and Carsten Maple, *Senior Member, IEEE*

***Abstract*—In intelligent transportation systems (ITS), communications between vehicles, i.e. vehicle-to-vehicle (V2V) communications are of greatest importance to facilitate autonomous driving. The current state-of-the-art for secure data exchange in V2V communications relies on public-key cryptography (PKC) consuming significant computational and energy resources for the encryption/decryption process and large bandwidth for the key distribution. To overcome these limitations, physical-layer security (PLS) has emerged as a lightweight solution by exploiting the physical characteristics of the V2V communication channel to generate symmetric cryptographic keys. Currently, key-generation algorithms are designed via empirical parameter settings, without resulting in optimum key-generation performance. In this paper, we devise a key-generation algorithm for PLS in V2V communications by introducing a novel channel response quantisation method that results in optimum performance via analytical parameter settings. Contrary to the current state-of-the-art, the channel responses incorporate all V2V channel attributes that contribute to temporal variability, such as three dimensional (3D) scattering and scatterers' mobility. An extra functionality, namely, Perturbe-Observe (PO), is further incorporated that enables the algorithm to adapt to the inherent non-reciprocity of the V2V channel responses at the legitimate entities. Optimum performance is evidenced via maximisation of the key bit generation rate (BGR) and key entropy (H) and minimisation of the key bit mismatch rate (BMR). A new metric is further introduced, the so-called secret-bit generation rate (SBGR), as the ratio of the number of bits which are successfully used to compose keys to the total amount of channel samples. SBGR unifies BGR and BMR and is thus maximised by the proposed algorithmic process.**

***Index Terms*—Cryptographic key generation, Physical layer security, Quantisation, Vehicular communications.**

I. Introduction

INTELLIGENT transportation systems (ITS) is an emerging technology that will facilitate various services such as collision avoidance, traffic jam management, infotainment, etc., to reduce transportation expenditure and enhance safety, security and level of comfort [1]. Communications between vehicles, i.e. vehicle-to-vehicle (V2V) communications and between vehicles and roadside infrastructure, i.e. vehicle-to-infrastructure (VI) communications constitute the backbone of ITS providing connectivity between all communication entities. Security is a top priority [2], [3] as the wireless medium opens up the possibility for unauthorised users to passively eavesdrop or to alter the transmissions [4]. Data confidentiality is traditionally provided by cryptographic mechanisms implemented in upper layers of the Open System Interconnection (OSI) model. Encryption approaches can be classified into two categories: symmetric (secret key) and asymmetric (public key) solutions [5].

The current state-of-the-art relies on public-key cryptography (PKC) to provide authentication, confidentiality, identity and non-repudiation. PKC primitives are computationally complex and vehicles' onboard units (OBUs) may still need hundreds of milliseconds to complete such operations, responsible for unacceptable delays when transmitting safety-related messages [6]. Furthermore, PKC is intrinsically a centralised approach, where a trusted authority distributes and manages keys and certificates, thus, its adaptation to highly distributed ad-hoc network raises scalability challenges [7]. On the other hand, symmetric cryptography is more computationally efficient than PKC but its applications are drastically limited by the delicate tasks of distributing and storing the secret keys. Distribution usually requires a secure secondary channel which is hardly feasible, especially in vehicular communication channels due to their rapid temporal variability and short-time connections [8].

In these challenging scenarios, Physical Layer Security (PLS) has emerged to provide unconditionally secure communications by efficiently exploiting the wireless medium as a shared source of randomness to extract symmetric keys [9]. PLS stems from the research of Wyner who demonstrated how it is possible to establish secure transmissions in scenarios where the eavesdropper (Eve) has a channel of lower quality than the communicating nodes (Alice and Bob) [10]. This difference of links' quality translates into a difference of channel capacities, referred to as secrecy capacity, which can be exploited to send private information. Maurer [11] and Ahlswede-Csiszar [12] demonstrated that confidentiality is also achievable when the attacker observes a higher quality link than the one available to authorised parties. This technique is based on the extraction of a secret key over the public and insecure channel.

Cryptographic keys are generated through the quantisation of channel response features, which are considered random

M. Bottarelli (mirko.bottarelli.1@warwick.ac.uk), G. Epiphaniou (Gregory.Epiphaniou@warwick.ac.uk) and C. Maple (cm@warwick.ac.uk) are with Secure Cyber Systems Research Group (SCSRG), Warwick Manufacturing Group (WMG), University of Warwick, UK.

P. Karadimas (petros.karadimas@glasgow.ac.uk) is with the James Watt School of Engineering, University of Glasgow, UK. P. Karadimas research was supported by the Engineering and Physical Sciences Research Council (EPSRC) under grant EP/R041660/1: Bandwidth and Energy Efficient Compact Multi-Antenna Systems for Connected Autonomous Vehicles.

D. Kbaier Ben Ismail (dhouha.kbaier@open.ac.uk) is with School of Computing & Communications, The Open University, UK.

processes, such as the Received Signal Strength (RSS) or the phase [13]. Randomness is a consequence of the unpredictability of the multipath propagation and nodes' mobility [14]. Nonetheless, successful key-generation is facilitated by the channel reciprocity principle, which states that in sufficiently small time-intervals, referred to as coherence time intervals, the channel response is substantially constant [14], [15]. Thus, the communicating parties can probe the channel in an interleaved fashion, obtaining similar estimates inside the same coherence time intervals, generating the same keys. Channel responses, obtained by illegitimate entities, are statistically uncorrelated to the legitimate ones, due to spatial and temporal variability of multipath propagation [14]. Thus, the generated keys are dissimilar compared to those of the legitimate entities and hence, communication data confidentiality is retained [5].

In the first phase of the key-extraction process, channel responses at the legitimate entities are quantised, in order to be converted to bit sequences [13]. This investigation focuses on the RSS quantisation for its ease of use and the immediate availability in all out-of-the-shelf wireless devices [16]. Furthermore, RSS-based quantisation greatly benefits from nodes' mobility, which is the major attribute of V2V communications, generating keys at a fast rate and with high entropy.

In their study, Tope et al. analysed the signal attenuation by collecting estimates of the envelope of received packets and storing them into arrays [17]. Two thresholds were used to drop estimates that have a high probability of being either foreseeable or converted to mismatching bits. In reference [18], deep fades or local minima of the signal are used to improve keys agreement. In this work, bitstreams are generated through a single threshold set by an automatic gain control circuit (AGC), to make it independent from the variability of signal power. Reference [19] introduced a quantiser with two thresholds, whose distance is proportional to the standard deviation of RSS estimates. The quantisation bin between thresholds is referred to as censor or invalid region, where values are dropped because of their high probability of disagreement. Furthermore, only the estimates located inside sequences of sufficient excursions above or below the thresholds are considered to discard sharp changes in the RSS. In reference [20], Adaptive Secret Bit Generation (ASBG) scheme refreshes the quantisation thresholds after each block of channel estimates. In its attempt to increase the bit generation, the scheme introduced multiple quantisation levels which, however, are severely limited by the noise and empirically set. Reference [21] used over-quantisation as an error-correcting technique for bit-disagreements. In fact, even if over-quantised bits are independent of the regular ones, they still remain correlated to legitimate parties. This amount of mutual information is then used to reduce the length of syndromes, increasing the overall generation rate. In [22], non-linear thresholds are used through the creation of a least-square polynomial curve, whose degree is empirically chosen according to the number of estimates and Doppler shift. The existing quantisation methods are designed through empirical settings of their parameters hence, they are not optimum by design. Interested readers are referred to [13] for a thorough survey on the performance and limitations of current state-of-the-art quantisation techniques. In this paper, we overcome this problem by using first and second order statistics, specifically the Cumulative Distribution Function (CDF) and the Average Fade Duration (AFD), in devising two novel quantisation methods thus, realising equal probability between 0s and 1s via analytical means.

The channel responses and hence the generated bit sequences at the legitimate entities are expected to be identical due to the reciprocity principle of wireless communication channels [14]. Hardware impairments, the noise inherent in communication channels and mainly, the half-duplex nature of the probing process causes discrepancies in the V2V channel responses and generated bit sequences at the legitimate entities [23]. All these effects are grouped into the term of imperfect reciprocity. Only a few algorithms in literature take the imperfect reciprocity into account. Half-duplex limitations are addressed in [24], [25] by applying fractional interpolation in order to measure estimates at the same time instants virtually. Moreover, non-reciprocity due to hardware differences is removed through a ranking method in [26]. In other studies [27], [28] non-reciprocity is simply ignored during quantisation and adequately tackled with error correction. Furthermore, to the best of our knowledge, there is no algorithm rigorously adaptable to the randomly varying reciprocity. In this paper, we compensate non-reciprocity component through the continuous adaptation of the quantisation thresholds.

Since a single different bit would make the generated keys unusable, the quantisation stage is often followed by an information reconciliation phase that rectifies bit discrepancies. A widely used technique is CASCADE in which parties randomly permute the sequences and recursively exchange parity check information [29]. More sophisticated schemes are based on turbo codes [27] and low-density parity-check (LDPC) [28] which both try to maximise reconciliation capabilities as well as, simultaneously minimise the leakage of information to the eavesdropper. Alice and Bob's sequences should now be identical; otherwise, the entire extraction process is restarted. However, to use such strings as keys, the last step of privacy amplification strengthens them by improving their entropy, for example, with the application of universal hash functions or one-way functions [30].

The performance of key-generation algorithms is quantified via standardised key performance metrics, namely, the bit generation rate (BGR), the bit mismatch rate (BMR) and the key entropy (H) [31]. BGR is defined as the number of bits that are generated per unit time or per channel sample. This is directly related to quantisation, however, it also evaluates the overall performance of the extraction process. In fact, higher BGRs allow the creation of keys in less time and this is crucial in low-latency V2V (safety) communications [32]. On the other hand, BMR measures the disagreement between the bit-streams obtained by the communicating parties. BMR is commonly defined after the quantisation stage and it indicates how the latter is susceptible to noise and imperfect reciprocity. However, in this paper, BMR is considered after information reconciliation to capture the performance of the complete key-generation process. By doing so, a high BMR indicates that the specific choice of quantisation parameters induces several mismatching bits that cannot be fully recovered by the chosen information reconciliation scheme. Finally, the entropy (H) of the extracted bit sequences measures their level of randomness [33]. The latter is a crucial property of cryptographic keys to remove possible statistical defects that could ease the attacks conducted by adversaries with active or passive presence to the channel [34].

What makes the design of key-generation algorithms challenging, is the conflicting relationship among the BGR, BMR and H of the resulting bitstreams. In their attempt to optimise the corresponding proposed schemes, most literature sources address only a subset of the metrics introduced above, coming up with sub-optimal results. BMR is the top priority metric to be addressed since any unrecoverable disagreement could lead to unusable keys [17], [18], [27]. In reference [17], thresholds are used to remove both predictable and erroneous bits, thus increasing entropy and decreasing BMR at the expense of a lower BGR. In [18], deep fades reduce BMR as well as BGR and H, further requiring the application of a fuzzy extractor to keep the entropy to a sufficient level. Moreover, all schemes try to improve the quantisation and information reconciliation independently, without considering their inner relationship. For example, reference [27] proposes a turbo codes-based reconciliation, using the same quantisation method initially proposed for the CASCADE protocol [29]. We address this challenge by introducing the novel metric of Secret Bit Generation Rate (SBGR) that facilitates the development of a thresholding optimisation algorithm, called Perturb-Observe (PO).

Secret-key establishment in V2V has been studied in [27], [35]–[40]. Reference [35] introduced two key-agreement algorithms for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) modes, respectively. In the first algorithm, quantisation is applied to the difference between two consecutive RSS values, instead of their absolute values. This way, the scheme can provide better results in static or slow-moving scenarios, while being resistant to RSS-manipulation attacks. In the second algorithm, random channel hopping creates the necessary frequency diversity, used to distribute secure seeds among road-side units. Reference [36] introduced vector quantisation to increase the bit generation. RSS estimates are reused n times, where n is the dimension of the vector and then sent to a fuzzy extractor, in order to achieve a zero bit-disagreement rate. While this approach could achieve better performances, it remains to investigate how estimates' recycling could reduce key robustness. References [37], [38] addressed two major challenges in extracting keys from vehicular environments, namely, the very short coherence time and the strong influence of noise. Both effects are addressed using sliding window smoothing, whose weights are collaboratively generated by Alice and Bob. V2V safety-related communications are delay-intolerant and require a reaction time of less than 100 milliseconds. Such a constraint has been considered in [39], where the authors designed a key-length optimisation algorithm. This algorithm attempts to extract a key with as much robustness as possible, starting from scenario's characteristics, such as parties' locations and an estimate of the coherence time. Reference [27] considers a parametric three-dimensional wireless propagation model, including scattering and scatterers' mobility. In such an environment, the channel non-reciprocity, which stems from channel noise and hardware impairments, is addressed with the application of turbo-codes. Results had demonstrated better key-generation rate and lower error-probability, compared to existing methods. Reference [40] analysed the feasibility of standard RSS-based algorithms in a generic vehicular stochastic model, considering latency and packet-size constraints. Even if the quantisation parameters were optimised empirically, primary findings showed that performances are still insufficient to support delay-intolerant services.

To summarise, the existing RSS-based algorithms fail to simultaneously optimise all the performance metrics (BGR, BMR and H). They do not consider the specific information reconciliation scheme in the choice of the quantisation parameters. Furthermore, those parameters are empirically set without taking into account the randomly varying non-reciprocity. To fill these gaps, our contributions are summarised as follows:

1) We prove the existence of optimal thresholding for the channel response employing a two-level, RSS-based quantisation scheme. We originally aim at having equiprobable 0s and 1s via analytical means. Accordingly, we make use of the Cumulative Distribution Function (CDF) and Average Fade Duration (AFD) statistics to mathematically create equiprobable regions, which in turn results in equiprobable 0s and 1s and eventually bit sequences with maximum H. Although the CDF has been employed in the past to partition the quantisation space [13], however, we use CDF to associate thresholds in order to dynamically generate equiprobable quantisation bins by design (not based on any empirical settings). The AFD is employed for the first time in this paper to define thresholds, and proved to outperform CDF-based thresholding in generated key randomness.
2) We define a new metric, named as Secret-Bit Generation Rate (SBGR) that accounts for the number of correct bits per channel sample. It represents an efficient comparator for different quantisation schemes, derived by considering both BMR and BGR. Besides, since we consider BMR after the information reconciliation stage, SBGR can evaluate quantisation performance as a function of the capabilities of the information reconciliation. In other words, SBGR allows for the adaptation of the proposed PO algorithm to every information reconciliation scheme.
3) We address the randomly varying non-reciprocity of the channel with the introduction of a novel Perturb-Observe (PO) algorithm. PO incorporates the Channel Gain Complement (CGC) [41] to mitigate non-reciprocity, as initially proposed in [27]. Furthermore, it acts as feedback in the key-extraction process, observing the SBGR performance to adjust quantisation thresholds accordingly. Thresholds can be continuously derived by the CDF and AFD statistics, which become adaptable to the V2V channel temporal variations, i.e. when CDF or ADF

change. As a result, the proposed algorithm outperforms the classical implementation of two-level quantisation derived from the mean and standard deviation (hereafter referred to as STD), as initially proposed in [19] and further employed in various articles published previously (among others [20], [27], [36], [39], [42], [43]). Table II shows that the proposed approaches provide faster key-generation rates (i.e., higher SBGR) than STD, while maintaining optimal entropy H.

The remaining of this paper is organised as follows: Section II presents the adopted V2V channel model and the key performance metrics. Section III presents the new analytical-based thresholding techniques and the proposed PO algorithm. Section IV presents results and comparisons with the standard thresholding technique STD [19]. Finally, Section V draws the conclusion.

II. Channel Model and Performance Metrics

We consider a highly-dense, non Line-of-Sight V2V communication scenario. In this challenging scenario, the received signal consists of the superposition of multipath components via the interaction with surrounding scatterers [44]. Such scatterers can be fixed and mobile (e.g. other vehicles) and such interaction contributes to the temporal variability of the V2V channel. Scatterers do not take part in the key-generation process, but they constitute wireless propagation mechanisms. Specifically, the impact of mobile scatterers is further incorporated via the model presented in [45].

Although systematic threat modelling is outside of the scope of this paper, however, we consider the malicious node Eve is able to eavesdrop the V2V communication channel without altering it. We also assume that Eve is located no less than half-wavelength from Alice or Bob. In fact, at greater distances, Eve perceives a statistically uncorrelated channel [46] thus, greatly reducing the probability of extracting the same key as the one used by legitimate parties.

A. V2V Stochastic Channel Model

To generate the most accurate synthetic data in our simulations, we employ a generic parametric stochastic channel model [44], which has proved to be applicable for key-generation [27]. This model considers the wireless channel response as a random process, the statistics of which provide insight into the V2V channel attributes.

Fig. 1 shows the considered three-dimensional V2V scenario, with propagation's parameters and entities' location. Two vehicles, Alice and Bob, are equipped with a single antenna and move at speeds $u_{A(B)}$. Alice's signals are received by Bob as the superposition of a number L of different echoes, unresolvable in delay. Each l-th multipath component reaches its destination with a specific complex amplitude a_l and phase ϕ_l caused by the different path it has travelled. These multipath components interact with a fixed or mobile scatterers [44].

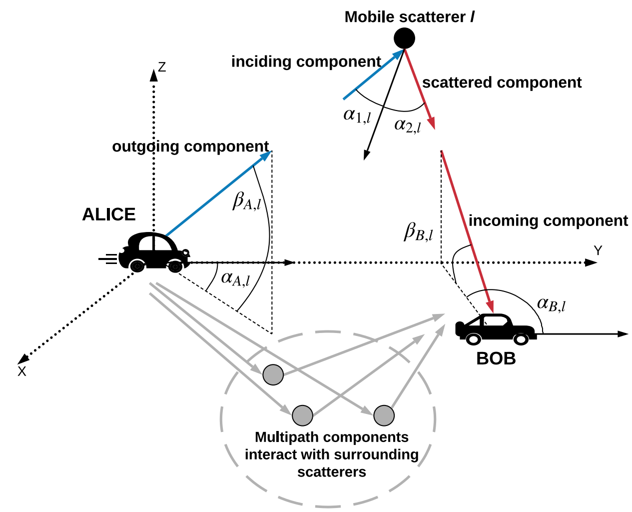


Fig. 1. V2V channel model: two vehicles are moving in a 3D multipath propagation environment including surrounding scatterers.

Alice's channel estimates G_A are generated by the following formula [44]:

$$G_A(t) = \sum_{l=1}^{L} |a_l| \exp(j\phi_l) \exp(j2\pi v_l t) \tag{1}$$

where t is the time and v_l the Doppler shift of the l-th multipath component. The latter is the sum of the contributions of the transmitter $v_{A,l}$, receiver $v_{B,l}$ and scatterers $v_{S,l}$, as follows:

$$v_l = v_{A,l} + v_{B,l} + v_{S,l} \tag{2}$$

$$v_{A(B),l} = u_{A(B)_{max}} \frac{f_c}{c} \cos\alpha_{A(B),l} \cos\beta_{A(B),l} \tag{3}$$

$$v_{S,l} = u_S \frac{f_c}{c} (\cos\alpha_{1,l} + \cos\alpha_{2,l}) \tag{4}$$

where $\alpha_{A(B),l}$ and $\beta_{A(B),l}$ are azimuth and elevation angles of departure (arrival) and $\alpha_{1,l}, \alpha_{2,l}$ are the incoming and outgoing angles at the mobile scatterer. Maximum Doppler shifts arise from nodes' mobility, having $u_{A(B)_{max}}$ the maximum velocities, λ the carrier's wavelength at frequency f_c and the speed of light c. The speed of mobile scatterers u_S is randomised through a Weibull distribution with scale and shape parameters w and a, respectively [44], [45]. Thus,

$$p_{u_S}(u_S) = w u_S^{a^{-1}} \exp(-w u_S^a / a) \tag{5}$$

Once we have Alice's estimates we need to properly generate the corresponding Bob's estimates in order to simulate the effects of imperfect reciprocity realistically. This loss of reciprocity is the direct consequence of slightly different channel state information (CSI) sensed by legitimate parties. In this study we mitigated the loss of reciprocity using the Channel Gain Complement (CGC) method [41]. The following parameters are estimated during a learning phase of M probes extracted by Alice $G_A(t_i)$ and Bob $G_B(t_i)$ inside the same coherence interval t_i

$$\mu = \frac{1}{M}\sum_{i=1}^{M}(G_A(t_i) - G_B(t_i)) \tag{6}$$

$$2\sigma_C^2 = \frac{1}{M}\sum_{i=1}^{M}(G_A(t_i) - G_B(t_i) - \mu)^2 \tag{7}$$

After subtracting μ from Alice's and Bob's time-domain channel responses, non-reciprocity is compensated, however, a zero-mean Gaussian distribution $N(0, 2\sigma_C^2)$ is still present as the difference between channel responses. Thus [41]

$$G_B(t) = G_A(t) + N(0, 2\sigma_C^2) \tag{8}$$

The impact of the noisy component usually depends on the environmental conditions, which are dynamic and unpredictable, especially in V2V communications. In this respect, our proposed algorithm aims to rapidly adapt quantisation thresholds to the available amount of channel non-reciprocity, modelled via the standard deviation σ_C.

B. Key Performance Metrics

In order to compare the proposed algorithm to the other schemes in the literature, it is necessary to introduce the performance metrics [31]. The quantisation performance is measured by the bit generation rate (BGR), which is the average number of bits that can be extracted per channel estimate or per unit time. The former definition is preferable, as it does not depend on the chosen probing rate. Thus

$$BGR = \frac{no.extracted\,bits}{no.channel\,samples} \tag{9}$$

Higher values of BGR indicate faster production of bit-streams which, in turn, translate to keys being generated in less time and hence refreshed continuously. Another relevant performance criterion is the bit-mismatch rate (BMR) defined as the ratio of the number of erroneous bits (i.e. they do not match between Alice and Bob) to the total amount of channel samples

$$BMR = \frac{no.erroneous\,bits}{no.channel\,samples} \tag{10}$$

BMR determines the algorithm's resilience against noise and interferences, defined after the quantisation stage or after the information reconciliation. In the first case, BMR depends only on how the quantisation space is modelled (as for example, the number of thresholds). On the other hand, if BMR is measured after information reconciliation, it accounts for the bits that cannot be successfully recovered by the chosen error-correcting approach. This way, BMR combines quantisation and reconciliation, allowing a holistic optimisation.

To simultaneously optimise BMR and BGR, we define a novel metric, namely the secret-bit generation rate (SBGR), as the ratio of the number of bits which are successfully used to compose keys to the total amount of channel samples that were used, thus

$$SBGR = \frac{no.secret\,bits}{no.channel\,samples} \tag{11}$$

Since BMR is defined after information reconciliation, the number of secret bits corresponds to the amount of successfully generated bits after information reconciliation, which can be expressed as

$$no.secret\,bits = no.samples \cdot BGR \cdot (1 - BMR) \tag{12}$$

By combining (11) and (12), we get

$$SBGR = BGR \cdot (1 - BMR) \tag{13}$$

Eq. (13) showcases how the new metric SBGR combines BGR and BMR. More specifically, SBGR is equal to BGR when all bits are correct hence, BMR = 0. Considering that the extracted sequences will be treated as cryptographic keys, it is important they possess enough average entropy, ideally close to 1, to maximise the uncertainty from an attacker's point of view. The entropy of bit i is measured by the following formula [27]:

$$H_i = -p_{0,i}\log p_{0,i} - (1 - p_{0,i})\log(1 - p_{0,i}) \tag{14}$$

where $p_{0,i}$ is the posterior probability of bit i being 0. The maximum value of 1 indicates the equal probability of having bits 1 or 0, i.e. $p_{1,i} = 1 - p_{0,i} = 0.5$. For independent bit-strings of length N, the average entropy is defined as $H_{avg} = (\sum_{i=1}^{N} H_i)/N$ [47]. Though a classical metric, entropy is not sufficient to prove the absence of statistical defects in the bit sequences. For example, they may contain long runs of the same bit and the repetition of sub-parts. For these reasons, in all our tests, we also evaluate key robustness against the random-tests suite, provided by the National Institute of Standards and Technology (NIST) [34].

III. Analytical Thresholding

Our quantisation scheme departs from work introduced in [19], where legitimate nodes locally convert their RSS-estimates in bit-streams, prior to symmetric key generation. Channel probing is done in half-duplex mode, hence Alice and Bob extract samples from the same coherence intervals in an interleaved fashion. The inability to probe at the same time instants introduces a small, yet unpredictable variation in the channel response [23]. The latter, together with other environmental factors, reduce the channel reciprocity as well as, increase the probability of extracting different key-candidates thus, they reduce the effectiveness of the extraction process. In order to reduce BMR, we apply a two-level "censor" quantisation function defined as follows:

$$Q(x) = \begin{cases} 1, & \text{if } x > q_+ \\ 0, & \text{if } x < q_- \\ \text{dropped} & \text{otherwise} \end{cases} \tag{15}$$

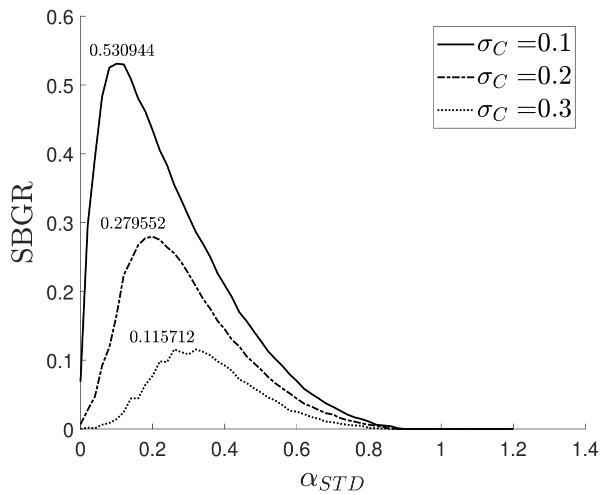


Fig. 2. SBGR against α_{STD} for different non-reciprocity factors in the standard censor approach.

TABLE I
SIMULATION PARAMETERS

Parameter	Value	Description
$DATASIZE$	50000	No. channel estimates
$RUNS$	120	No. test runs
L	20	No. multipaths components
$u_{A(B)max}$	30 m/s (108 km/h)	Transmitter (receiver) max speeds
$u_{S_{max}}$	30 m/s (108 km/h)	Scatterers' max speed
$\alpha_{A(B),l}$	$U[-\pi, +\pi]$	Azimuth angles of departure (arrival)
$\beta_{A(B),l}$	$U[0, \pi/3]$	Elevation angles of departure (arrival)
$\alpha_{1,l}, \alpha_{2,l}$	$U[-\pi, +\pi]$	Scatterers' incoming/outgoing angles
f_c	6 GHz	Carrier frequency
w	2.958	Weibull scale parameter
a	0.428	Weibull shape parameter

Estimates in the interval $q_- \leq x \leq q_+$ are dropped in accordance with their higher probability of being translated into different bits at both communication ends. On the other hand, the censor region has a direct impact of the performance of the quantisation stage and its size should be set as the optimal trade-off between BMR and BGR metrics. Authors in [19] introduced a technique where thresholds were initially computed using average and standard deviation of an array of RSS samples $\underline{h}$, thus

$$q_{\pm} = average(\underline{h}) \pm \alpha_{STD} \cdot stdev(\underline{h}) \tag{16}$$

where parameter α_{STD} accounts for the size of the censor region and is calculated empirically. That technique has been extensively employed in the published state-of-the-art [20], [27], [36], [39], [42], [43]. Fig. 2 shows SBGR against different invalid region sizes modelled through the parameter α_{STD} in eq. (16) and for different non-reciprocity settings, represented by the standard deviation σ_C in eq. (7). SBGR performance increases as channel non-reciprocity (σ_C) reduces. Simulation parameter setting is shown in Table I.

Given the fact that all curves in Fig. 2 express a single (global) maximum, a Hill climbing algorithm seems to be a simple yet effective approach to locate the point with the highest performance [48, Ch. 7]. The idea is to "modulate" the quantisation thresholds, according to the resulting SBGR, in an attempt to identify the optimal set-point. However, as stated in the introduction, a high entropy H of the generated bit-streams is a mandatory requirement to guarantee the statistical robustness of the resulting symmetric keys. As the definition of SBGR does not ensure maximum entropy, we will relate the thresholds to achieve maximum entropy via analytical means.

A. CDF-based Thresholding Strategy

The first proposed strategy is based on the cumulative distribution function (CDF) $F_X(\cdot)$. In the case of two-level quantisation, optimal key-entropy is guaranteed by forcing thresholds $q_{\pm}$ to generate equiprobable regions, thus

$$\begin{aligned} F_X(q_-) &= Pr(-\infty < x \leq q_-) \\ &= Pr(q_+ \leq x < +\infty) \\ &= 1 - F_X(q_+) \end{aligned} \tag{17}$$

In the absence of a line-of-sight (LOS) component, the Rayleigh distribution is adopted as an example in this paper [44]. Its CDF is defined as follows:

$$F_X(x) = 1 - \exp(-\frac{x^2}{2\sigma^2}) \tag{18}$$

By combining eqs. (17) and (18) and after some algebraic manipulations, we derive the upper threshold with respect to the lower as

$$q_+ = \sqrt{2}\sigma \sqrt{\log\left(\frac{1}{1 - \exp(-\frac{q_-^2}{2\sigma^2})}\right)} \tag{19}$$

B. AFD-based thresholding strategy

The second proposed method is based on the use of average fade duration (AFD), a second-order statistical parameter, which could better capture channel temporal variability and simultaneously maintain a sufficient level of key robustness. AFD is defined as [49, pp 79-81]:

$$T(z) = F_X(z)/N(z) \tag{20}$$

that is the ratio between the cumulative distribution function and the level crossing rate (LCR) $N(\cdot)$. In Rayleigh environments, LCR is expressed by the following formula [44]:

$$N(z) = \sqrt{\frac{d_1}{2\pi}} \exp(-\frac{z^2}{2\sigma^2}) \frac{z}{\sigma^2} \tag{21}$$

where parameter d_1 depends on vehicles' speeds and multipath angular spread (see [44] for details). The core concept of using AFD is to ensure that when a signal crosses a threshold, it will remain in the corresponding region for the same (averaged) time duration. Mathematically,

$$T(q_-) = T^c(q_+) \tag{22}$$

where $T^c(z) = (1 - F_X(z))/N(z)$ is also commonly referred to as connection time. Thus, we have from (20)

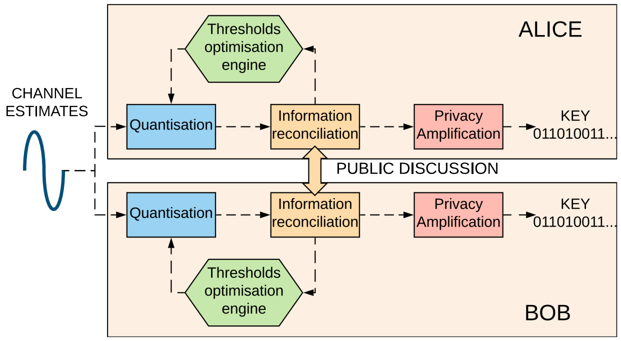


Fig. 3. Thresholds optimisation block acts as a feedback in PLS key-generation process.

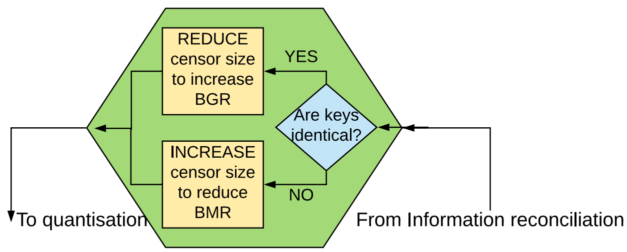


Fig. 4. A simplified view of the optimisation block: reconciliation outcome is used to adapt thresholds distance.

$$\begin{aligned} T(q_-) &= \frac{1-\exp(-\frac{q_-^2}{2\sigma^2})}{\sqrt{\frac{d_1}{2\pi}}\exp(-\frac{q_-^2}{2\sigma^2})\frac{q_-}{\sigma^2}} \\ &= \frac{\exp(-\frac{q_+^2}{2\sigma^2})}{\sqrt{\frac{d_1}{2\pi}}\exp(-\frac{q_+^2}{2\sigma^2})\frac{q_+}{\sigma^2}} \\ &= T^c(q_+) \end{aligned} \tag{23}$$

Using (18) and (21) in (23) and after some algebraic manipulations we get

$$q_+ = \frac{q_-}{\exp(\frac{q_-^2}{2\sigma^2})-1} \tag{24}$$

Whenever it is needed to adapt the quantisation thresholds, the two proposed strategies provide an analytical way to derive the thresholds and invalid region's boundaries, enforcing maximum entropy as well as facilitating a novel optimisation block using the SBGR metric.

C. Thresholding Optimisation

In this section we introduce an optimisation block in the standard process of key extraction to realise the maximum SBGR performance of the algorithm without relying on the choice of fixed quantisation parameters. Fig. 3 shows that the novel block acts as feedback from the information reconciliation scheme to adapt the quantisation parameters by continuously monitoring the output of the bit-extraction process. Inside this block, a Perturb-Observe (PO) algorithm constantly alters the invalid region size and monitors the effects on the resulting SBGR. In doing so, PO can adapt to different scenarios of channel non-reciprocity. For the sake of simplicity, the algorithm perturbs the size of the censor region by a positive amount $\delta > 0$, acting on the lower threshold q_- and leaving the corresponding upper threshold q_+ computed accordingly to the chosen strategy (CDF-based or AFD-based). Fig. 4 shows the intuitive underlying idea: if the generated bitstreams are different after reconciliation, this indicates increased channel non-reciprocity (σ_C increases), which should be balanced by a larger censor region. On the other hand, matching keys suggest the possibility to reduce thresholds' distance further, thus, aiming for higher BGR.

The frequency with which the thresholds should be perturbed must be carefully chosen: if thresholds are modulated too often, they can generate a significant oscillation around the optimal SBGR, preventing complete convergence. On the other hand, if the algorithm does not calibrate itself fast enough, it may not be able to reach optimality before the wireless channel has moved to a different non-reciprocity condition. To strike a balance, it seems reasonable to perturb quantisation bins after a minimum number of events. More specifically, the algorithm waits for a number $INT_{SUCCESS}$ of successful keys before reducing the censor size and a number of INT_{FAIL} failed attempts before increasing it. Usually $INT_{FAIL} \leq INT_{SUCCESS}$ because it is safer to faster adapt to worse conditions than to improve already good ones.

The PO algorithm reaches the highest SBGR point, where perturbance should be stabilised in order to avoid changes to the thresholds distance that can lead to bits discarded or rejection of keys. For that reason, the algorithm simultaneously quantifies the channel estimates against three pairs of thresholds $q_\pm^{(1)}, q_\pm^{(2)}, q_\pm^{(3)}$ whose lower parts are spaced by $\delta > 0$, thus

$$q_-^{(1)} = q_-^{(2)} + \delta \tag{25}$$

$$q_-^{(3)} = q_-^{(2)} - \delta \tag{26}$$

Considering that eqs. (19) and (24) are monotonically decreasing functions (see Appendix A), the three regions are in the following order relation

$$(q_+^{(1)} - q_-^{(1)}) \leq (q_+^{(2)} - q_-^{(2)}) \leq (q_+^{(3)} - q_-^{(3)}) \tag{27}$$

Recalling that smaller regions generate higher BGR as well as higher BMR, we will refer to those pairs hereafter as aggressive thresholds $q_\pm^{(1)}$, neutral thresholds $q_\pm^{(2)}$ and defensive thresholds $q_\pm^{(3)}$ which will be further evaluated in this specific order.

Fig. 5 shows the complete algorithm flowchart which can be best explained by considering three possible conditions: firstly, the algorithm is using a censor region's size which is larger than the optimal one for the current reciprocity factor. In that case, it is highly probable that aggressive thresholds $q_\pm^{(1)}$ will be adequate to generate keys successfully. If this condition is held for $INT_{SUCCESS}$ times, it is reasonable to

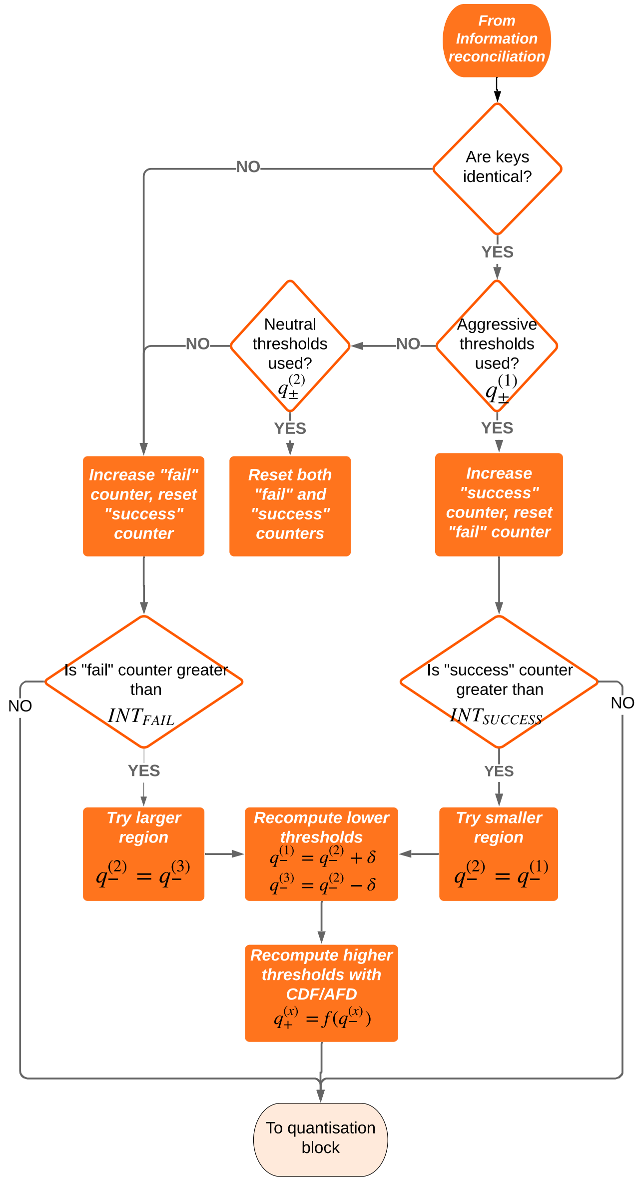


Fig. 5. Flowchart of PO algorithm where quantisation thresholds are adjusted to achieve the maximum key-generation rate.

consider these thresholds as neutral, assigning $q_-^{(2)} = q_-^{(1)}$. Secondly, when the algorithm reaches the maximum SBGR and channel reciprocity is stable, it is more likely that neutral thresholds $q_{\pm}^{(2)}$ will be valid, leaving all parameters unchanged as in the previous attempt, thus avoiding oscillations. Finally, if we assume that the algorithm is using a smaller censor region concerning the current channel condition, only defensive thresholds $q_{\pm}^{(3)}$ are probably valid or else none, suggesting a shift $q_-^{(2)} = q_-^{(3)}$ after INT_{FAIL} occurrences. Finally, $q_-^{(2)}$ is used to recalculate the other lower thresholds according to eqs. (25), (26) and, hence, the corresponding upper ones through eqs. (19), (24).

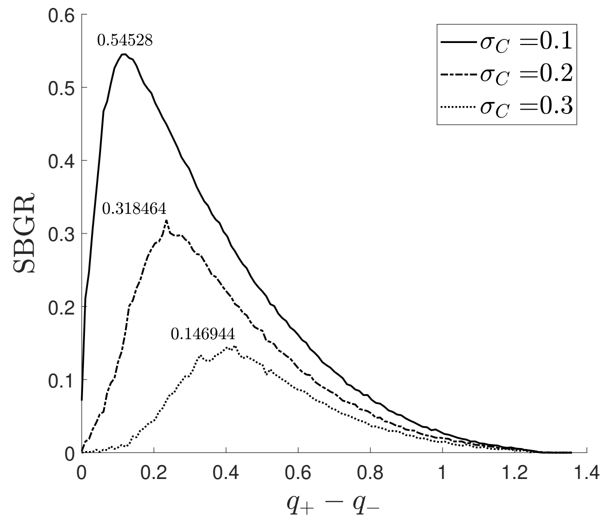


Fig. 6. CDF-thresholding strategy for different non-reciprocity factors.

IV. Simulations and Results

During the tests, simulations have been generated using Monte Carlo technique [50], [51]. Every simulation included 50,000 channel estimates, repeated for 120 runs to stabilise the resulting statistics. Furthermore, the number of multipath components was $L = 20$ to recreate a purely diffuse Rayleigh environment, capable of modelling an urban scenario. Since estimates have to be collected from uncorrelated different coherence region of duration T_{coh}, we used a fixed maximum probing rate $F_p = 1/T_{coh}$ where $T_{coh} = 1/v_{max}$ with $v_{max} = (u_{A_{max}} + u_{B_{max}} + 2u_{S_{max}})/\lambda$ the maximum Doppler shift [44]. See Table I for the parameter settings.

In the first set of experiments, we evaluated the performance of the new thresholding strategies. A standard two-level quantisation scheme [19] with CASCADE has been modified to analytically derive the thresholds using CDF and AFD-based formulae presented in section III. Figs. 6 and 7 show SBGR performances against censor size for different non-reciprocity configurations modelled by the standard deviation σ_C. Results are summarised in Table II, where both approaches outperform STD in all scenarios, especially with worse reciprocity. Performances are substantially equivalent, where CDF scores slightly better results in correspondence to $\sigma_C = 0.20$ and $\sigma_C = 0.30$, whilst AFD results superior in all other setups. According to Eq. 11, SBGR expresses the number of bits which can be extracted on average from each channel sample. Also, SBGR counts the number of mutually agreeable bits between Alice and Bob. These bits are candidates for the final key generated. Table II also shows the number of keys (128-bits) which were successfully generated using the full data-size of 50,000 probes with each technique. The same Table also illustrates how both analytical strategies are able to generate high entropy keys, even in low reciprocity environments ($\sigma_C = 0.30$), where STD fails to do so. Therefore, our approach outperforms the widely employed STD quantisation technique.

In the second set of experiments, accuracy and performance of the PO algorithm have been evaluated through extensive

TABLE II
RESULTING SBGR, ENTROPY AND NUMBER OF 128-BIT KEYS OF STD, CDF AND AFD APPROACHES

σ_C	STD			CDF			AFD		
	SBGR	H	Keys	SBGR	H	Keys	SBGR	H	Keys
0.10	0.5309	0.9935	207	0.5453 (+2.71%)	0.9947	213	0.5504 (+3.76%)	0.9941	215
0.15	0.4122	0.9933	161	0.4188 (+1.60%)	0.9937	164	0.4270 (+3.59%)	0.9941	167
0.20	0.2796	0.9934	109	0.3185 (+13.91%)	0.9940	124	0.3072 (+9.87%)	0.9932	120
0.25	0.1946	0.9934	76	0.2068 (+6.27%)	0.9939	81	0.2140 (+9.97%)	0.9925	84
0.30	0.1157	0.5252	45	0.1469 (+26.97%)	0.9942	57	0.1423 (+22.99%)	0.9920	56

TABLE III
RESULTS OF NIST TESTS ON THE PO ALGORITHM WITH CDF AND AFD THRESHOLDING STRATEGIES

Test (128-bit keys)	PO-CDF			PO-AFD		
	$\sigma_C = 0.10$	$\sigma_C = 0.20$	$\sigma_C = 0.30$	$\sigma_C = 0.10$	$\sigma_C = 0.20$	$\sigma_C = 0.30$
monobit	0.7798	0.0736	0.0292	0.4338	0.8230	0.1312
frequency	0.7328	0.5190	0.0336	0.8197	0.9705	0.4008
runs	0.9982	0.9374	0.1211	0.8096	0.3412	0.8604
longest run ones	0.0610	0.6601	0.9287	0.4793	0.6442	0.7589
dft	0.3049	0.7975	0.3049	0.7975	0.4416	0.6079
non overlapping template matching	0.9996	0.9931	0.8218	0.9935	0.9373	0.5865
serial	0.4731	0.5528	0.0321	0.2649	0.5620	0.2867
approximate entropy	0.5468	0.5719	0.0326	0.6215	0.8187	0.2970
cumulative sums	0.8982	0.0471	0.0113	0.5492	0.7797	0.1075
random excursions	0.0158	0.0001	0.0018	0.0238	0.0957	0.0445
random excursions variant	0.0514	0.0005	0.1597	0.0593	0.0156	0.1991

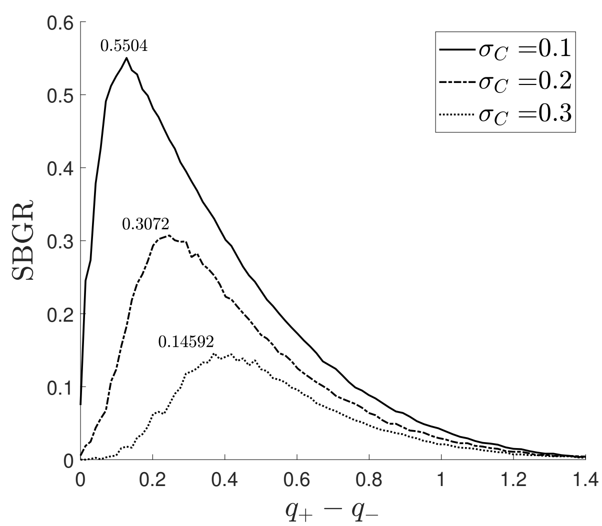


Fig. 7. AFD-thresholding strategy for different non-reciprocity factors.

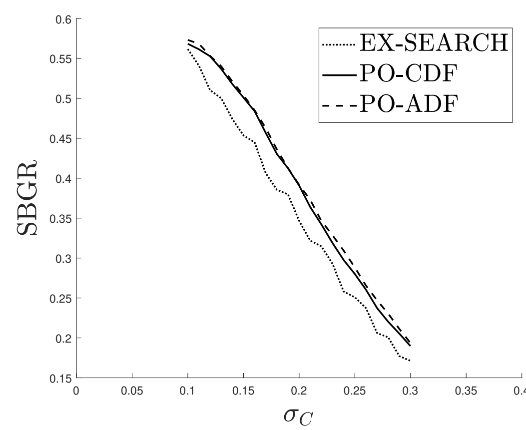


Fig. 8. Performance of Perturb-Observe algorithm compared to exhaustive search.

simulation. As the baseline, we introduced a quantisation scheme, referred to as EX-SEARCH, where the thresholds are chosen directly from a lookup table. The latter has been created through an exhaustive search, containing the optimal thresholds for various non-reciprocity settings in the range $\sigma_C \in [0.10, 0.30]$. Fig. 8 shows the PO algorithm's performance against EX-SEARCH. CDF and AFD configurations provide similar results, however, they both outperform EX-SEARCH, emphasising the superiority of our self-configurable approach. Improvements have been made due to the PO's ability to adapt and exploit the time intervals, where the random estimates temporally allow for a smaller censor-size hence, a higher BGR.

In the last set of experiments, we applied the NIST test suite [34] to the bitstreams generated by our algorithm in order to prove the absence of statistical defects. Each test returns a P-value indicating the strength of the evidence against the null hypothesis. More specifically, when the returned P-value is larger than the chosen significance level ($\alpha_{sig} = 0.01$), the sequence can be considered as random. Nonetheless, four tests, namely 'Binary Matrix Rank', 'Overlapping Template Matching', 'Maurers Universal' and 'Linear Complexity', require extremely long streams, which cannot be provided by this specific simulator and hence they were excluded. Table 3 shows the P-values of the different tests for different reciprocity conditions. CDF-based thresholding has occasionally failed the 'random excursions' tests in case of low channel reciprocity, whilst AFD-based thresholding proved to be always successful. A possible explanation is that AFD, being a second order channel statistic, can potentially capture better the channel temporal dynamics.

V. Conclusion

In this paper, we derived new analytical formulas for the quantisation thresholds in secret key extraction algorithms using V2V channel responses in the time domain. We employed three-dimensional stochastic channel modelling, including the impact of mobile scatterers. Advancing the current-state-of-the-art, the proposed CDF- and AFD-based analytical thresholding techniques guarantee entropy maximisation of the resulting keys. With the aid of such techniques, we introduced a quantisation optimisation block, named as PO algorithm, as feedback in the key generation process to combat non-reciprocity between the channel responses. The proposed approach can be applied to any wireless propagation scenario, although our focus was on V2V communications. Better overall performance was demonstrated via the induction of a new metric, i.e., the SBGR. The proposed PO algorithm can adapt to varying reciprocity conditions, which makes it unaffected from empirical choices of parameters that do not secure optimum performance. Robustness of the generated keys was tested evaluating their respective Shannon entropies as well as, against the NIST tests suite. In both cases, the resulting bit sequences were proved sufficiently random. Through our extensive simulations, the AFD-based thresholding strategy has emerged as the suitable candidate for the generation of high-quality high-diversity cryptographic keys, exploiting and tracking the inherent time-domain randomness. Finally, part of our current research activities seek to explore the efficacy of additional information reconciliation schemes and their impact upon the overall key generation performance, using the proposed PO algorithm.

Appendix A

Considering $q_+ = f_1(q_-)$ in eq. (19), the first order derivative will be

$$\begin{aligned}\frac{d}{dq_-}f_1(q_-) &= \\ &= \frac{d}{dq_-}\left(\sqrt{2}\sigma\sqrt{\log\left(\frac{1}{1-\exp(-\frac{q_-^2}{2\sigma^2})}\right)}\right) \\ &= -\frac{q_-\exp(-\frac{q_-^2}{2\sigma^2})}{\sqrt{2}\sigma(1-\exp(-\frac{q_-^2}{2\sigma^2}))\sqrt{\log\left(\frac{1}{1-\exp(-\frac{q_-^2}{2\sigma^2})}\right)}}\end{aligned} \tag{28}$$

Since all factors in both numerator and denominator are positive for $q_- > 0$ and $\sigma > 0$, the first derivative is always negative hence, $f_1(q_-)$ and eq. (19) are monotonically decreasing functions.

We now consider $q_+ = f_2(q_-)$ in eq. (24), having the following first order derivative

$$\begin{aligned}\frac{d}{dq_-}f_2(q_-) &= \\ &= \frac{d}{dq_-}\left(\frac{q_-}{\exp(\frac{q_-^2}{2\sigma^2})-1}\right) \\ &= \frac{1}{\exp(\frac{q_-^2}{2\sigma^2})-1} - \frac{q_-^2\exp(\frac{q_-^2}{2\sigma^2})}{\sigma^2(\exp(\frac{q_-^2}{2\sigma^2})-1)^2} \\ &= -\frac{\sigma^2+q_-^2\exp(\frac{q_-^2}{2\sigma^2})-\sigma^2\exp(\frac{q_-^2}{2\sigma^2})}{\sigma^2(\exp(\frac{q_-^2}{2\sigma^2})-1)^2}\end{aligned} \tag{29}$$

where the denominator is always positive. Considering the numerator in eq. (29) we prove that is always positive. Thus

$$q_-^2\exp(\frac{q_-^2}{2\sigma^2})-\sigma^2\exp(\frac{q_-^2}{2\sigma^2}) \geq 0 \tag{30}$$

After some elementary algebraic manipulations, inequality (30) becomes

$$\frac{1}{\exp(\frac{q_-^2}{2\sigma^2})}+\frac{q_-^2}{\sigma^2} \geq 1 \tag{31}$$

Setting $q_-^2/\sigma^2 = x$, $x \geq 0$, we have

$$\frac{1}{\exp(x/2)}+x \geq 1 \tag{32}$$

Considering $g(x) = \frac{1}{\exp(x/2)}+x$, the first order derivative will be

$$\begin{aligned}\frac{d}{dx}g(x) &= \\ &= \frac{d}{dx}\left(\frac{1}{\exp(x/2)}+x\right) \\ &= 1-\frac{\exp(-x/2)}{2}\end{aligned} \tag{33}$$

We have $g(0) = 1$. Moreover, from eq. (33) the derivative is always positive. Thus, $g(x)$ is a monotonically increasing function, verifying the validity of ineq. (32) which, in turn, verifies ineq. (30). This makes $f_2(q_-)$ and eq. (24) monotonically decreasing functions.

References

[1] F. J. Martinez, C. Toh, J. Cano, C. T. Calafate, and P. Manzoni, "Emergency services in future intelligent transportation systems based on vehicular communication networks," *IEEE Intelligent Transportation Systems Magazine*, vol. 2, no. 2, pp. 6–20, 2010.

[2] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Vanet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7 – 20, 2017.

[3] L. Gafencu, L. Scripcariu, and I. Bogdan, "An overview of security aspects and solutions in vanets," in *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*, 2017, pp. 1–4.

[4] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[5] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*, 1st ed. USA: CRC Press, Inc., 1996.

[6] E. C. Eze, S.-J. Zhang, E.-J. Liu, and J. C. Eze, "Advances in vehicular ad-hoc networks (vanets): Challenges and road-map for future development," *Int. J. Autom. Comput.*, vol. 13, no. 1, p. 1–18, Feb. 2016.

[7] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, “Internet of things security: A top-down survey,” *Computer Networks*, vol. 141, pp. 199 – 221, 2018.

[8] M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on vanet security challenges and possible cryptographic solutions,” *Vehicular Communications*, vol. 1, no. 2, pp. 53 – 66, 2014.

[9] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[10] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[11] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[12] R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography. i. secret sharing,” *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[13] M. Bottarelli, G. Epiphaniou, D. K. B. Ismail, P. Karadimas, and H. Al-Khateeb, “Physical characteristics of wireless communication channels for secret key establishment: A survey of the research,” *Computers & Security*, vol. 78, pp. 454 – 476, 2018.

[14] G. Durgin, *Space-Time Wireless Channels*, 1st ed. USA: Prentice Hall Press, 2002.

[15] G. S. Smith, “A direct derivation of a single-antenna reciprocity relation for the time domain,” *IEEE Transactions on Antennas and Propagation*, vol. 52, no. 6, pp. 1568–1577, 2004.

[16] Y. E. H. Shehadeh and D. Hogrefe, “A survey on secret key generation mechanisms on the physical layer in wireless networks,” *Sec. and Commun. Netw.*, vol. 8, no. 2, p. 332–341, Jan. 2015.

[17] M. A. Tope and J. C. McEachen, “Unconditionally secure communications over fading channels,” in *2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No.01CH37277)*, vol. 1, 2001, pp. 54–58 vol.1.

[18] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, “Robust key generation from signal envelopes in wireless networks,” in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS ’07. New York, NY, USA: Association for Computing Machinery, 2007, p. 401–410.

[19] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, *Secret Key Extraction from Level Crossings over Unauthenticated Wireless Channels*. Boston, MA: Springer US, 2010, pp. 201–230.

[20] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, “On the effectiveness of secret key extraction from wireless signal strength in real environments,” in *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom ’09. New York, NY, USA: Association for Computing Machinery, 2009, p. 321–332.

[21] M. Yuliana, Wirawan, and Suwadi, “Performance evaluation of the key extraction schemes in wireless indoor environment,” in *2017 International Conference on Signals and Systems (ICSigSys)*, 2017, pp. 138–144.

[22] D. S. Karas, G. K. Karagiannidis, and R. Schober, “Neural network based phy-layer key exchange for wireless communications,” in *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*, 2011, pp. 1233–1238.

[23] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key generation from wireless channels: A review,” *IEEE Access*, vol. 4, pp. 614–626, 2016.

[24] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, “High-rate uncorrelated bit extraction for shared secret key generation from channel measurements,” *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.

[25] Hongbo Liu, Jie Yang, Yan Wang, and Yingying Chen, “Collaborative secret key extraction leveraging received signal strength in mobile wireless networks,” in *2012 Proceedings IEEE INFOCOM*, 2012, pp. 927–935.

[26] J. Croft, N. Patwari, and S. K. Kasera, “Robust uncorrelated bit extraction methodologies for wireless sensors,” in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, ser. IPSN ’10. New York, NY, USA: Association for Computing Machinery, 2010, p. 70–81.

[27] G. Epiphaniou, P. Karadimas, D. Kbaier Ben Ismail, H. Al-Khateeb, A. Dehghantanha, and K. R. Choo, “Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social iot networks,” *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2496–2505, 2018.

[28] S. Baksi, J. Snoap, and D. C. Popescu, “Secret key generation using one-bit quantized channel state information,” in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, 2017, pp. 1–6.

[29] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” in *Advances in Cryptology - EUROCRYPT ’93*, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[30] R. Impagliazzo, L. A. Levin, and M. Luby, “Pseudo-random Generation from One-way Functions,” in *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, ser. STOC ’89. New York, NY, USA: ACM, 1989, pp. 12–24.

[31] T. Wang, Y. Liu, and A. V. Vasilakos, “Survey on channel reciprocity based key establishment techniques for wireless systems,” *Wirel. Netw.*, vol. 21, no. 6, p. 1835–1846, Aug. 2015.

[32] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, “Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions,” *IEEE Communications Surveys Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[33] C. E. Shannon, “A Mathematical Theory of Communication,” *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul 1948.

[34] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. April, 2010.

[35] B. Zan, M. Gruteser, and F. Hu, “Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 8, pp. 4020–4027, 2013.

[36] X. Li, J. Liu, Q. Yao, and J. Ma, “Efficient and consistent key extraction based on received signal strength for vehicular ad hoc networks,” *IEEE Access*, vol. 5, pp. 5281–5291, 2017.

[37] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, “Extracting secret key from wireless link dynamics in vehicular environments,” in *2013 Proceedings IEEE INFOCOM*, 2013, pp. 2283–2291.

[38] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li and G. Chen, “Using wireless link dynamics to extract a secret key in vehicular scenarios,” *IEEE Transactions on Mobile Computing*, vol. 16, no. 7, pp. 2065–2078, 2017.

[39] J. Wan, A. Lopez, and M. A. A. Faruque, “Physical layer key generation: Securing wireless communication in automotive cyber-physical systems,” *ACM Trans. Cyber-Phys. Syst.*, vol. 3, no. 2, Oct. 2018.

[40] M. Bottarelli, G. Epiphaniou, D. K. Ben Ismail, P. Karadimas, and H. Al-Khateeb, “Quantisation feasibility and performance of RSS-based secret key extraction in VANETs,” in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, Jun 2018, pp. 1–8.

[41] H. Liu, Y. Wang, J. Yang, and Y. Chen, “Fast and practical secret key extraction by exploiting channel response,” in *2013 Proceedings IEEE INFOCOM*. IEEE, apr 2013, pp. 3048–3056.

[42] Wei Xi, Xiang-Yang Li, Chen Qian, Jinsong Han, Shaojie Tang, Jizhong Zhao, and Kun Zhao, “Keep: Fast secret key extraction protocol for d2d communication,” in *2014 IEEE 22nd International Symposium of Quality of Service (IWQoS)*, 2014, pp. 350–359.

[43] S. T. Ali, V. Sivaraman, and D. Ostry, “Zero reconciliation secret key generation for body-worn health monitoring devices.” New York, NY, USA: Association for Computing Machinery, 2012.

[44] P. Karadimas and D. Matolak, “Generic stochastic modeling of vehicle-to-vehicle wireless channels,” *Vehicular Communications*, vol. 1, no. 4, pp. 153–167, 2014.

[45] P. Karadimas, E. D. Vagenas, and S. A. Kotsopoulos, “On the scatterers’ mobility and second order statistics of narrowband fixed outdoor wireless channels,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 7, pp. 2119–2124, 2010.

[46] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy,” *Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom ’08*, p. 128, 2008.

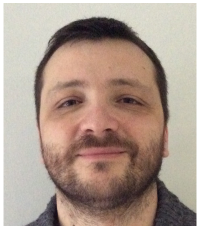
[47] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley, sep 2005.

[48] S. S. Skiena, *The Algorithm Design Manual*. Springer London, 2008.

[49] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[50] P. Hirschausen, L. M. Davis, D. Haley, and K. Lever, “Identifying key design parameters for Monte Carlo simulation of Doppler spread channels,” *2014 Australian Communications Theory Workshop, AusCTW 2014*, pp. 33–38, 2014.

[51] P. Hoeher, "A Statistical Discrete-Time Model for the WSSUS Multipath Channel," *IEEE Transactions on Vehicular Technology*, vol. 41, no. 4, pp. 461–468, 1992.



Mirko Bottarelli Mr. Mirko Bottarelli was born in 1980 in Milan, Italy. He received his Bachelor and Master's degrees in Computer Science from Università degli Studi di Milano Bicocca, Milan, Italy in 2004 and 2006, respectively. He is a lecturer in Cybersecurity in the Faculty of Mathematics and Computer Science at the University of Wolverhampton. Being a member of the Order of Engineers in Italy and a software architect and engineer, he is currently pursuing a PhD degree in the Warwick Manufacturing Group (WMG), University of Warwick, UK. His research interests are in the area of wireless communication, information theory and physical layer security. He is also interested in blockchain technologies and other related areas.

Petros Karadimas Dr. Petros Karadimas completed his MEng and PhD degrees in the Department of Electrical and Computer Engineering, University of Patras, Greece, in 2002 and 2008, respectively. He was a Research Fellow in the Centre for Wireless Network Design (CWIND), University of Bedfordshire, UK, from December 2009 until August 2011. He was appointed as a Lecturer in Electronic Engineering in the same University in September 2011. In August 2016, he moved to the University of Glasgow, UK, as a Lecturer in Electrical and Electronic Engineering, where he established a research group focusing on antenna arrays and MIMO antennas design and optimization. He also led the development and establishment of the Communications Sensing and Imaging (CSI) theme as part of the Systems, Power and Energy (SPE) research division of the James Watt School of Engineering. He has received funding by major research councils and organizations including UK's EPSRC and CDE/DSTL. His broad research interests include: a) Radio Propagation and Wireless Channel Modeling, b) Antenna Arrays and MIMO Antennas, c) Communication and Information Theory and d) Physical Layer Wireless Security and Secrecy.

Gregory Epiphaniou Currently holds a position as an Associate Professor of security engineering in WMG's Secure Cyber Systems Research Group at the University of Warwick. His role involves bid support, applied research and publications. He led and contributed to several research projects funded by EPSRC, IUK and local authorities totalling over £3M. He is also the main inventor of a patented-pending technology on a distributed ledger system (GB2576160A/US200042497A1). He was previously holding a position as a Reader in Cybersecurity and acted as deputy director of the Wolverhampton Cybersecurity Research Institute (WCRI). He has taught in many universities both nationally and internationally a variety of areas related to proactive network defence with over 80 international publications in journals, conference proceedings and author in several books and chapters. He holds several industry certifications around Information Security and worked with several government agencies including the UK MoD in Cybersecurity related projects. He currently holds a subject matter expert panel position in the Chartered Institute for Securities and Investments. He acts as a technical committee member for several scientific conferences in Information and network security and serves as a key member in the development of WS5 for the formation of the UK Cybersecurity Council.

Dhouha Kbaier Ben Ismail Since 2018, Dr Dhouha Kbaier is a senior lecturer in Computer Networking and an active research member of the Wolverhampton Cyber Research Institute (WCRI) in the Faculty of Science and Engineering at the University of Wolverhampton. She received from Telecom Bretagne (Brest, France) both her PhD in 2011 with the highest honours and her Master of Engineering degree in 2008. She was specialised in Space Communications Systems in the French "Grande École" ISAE in Toulouse, heart of the European Aerospace Industry. Prior to working at the University of Wolverhampton, she joined the University of Bedfordshire as a Lecturer in Telecommunications and Network Engineering in 2016. She also worked for several years as a post-doctoral research follower first at Telecom Bretagne, then with Thales Airborne Systems and finally at IFREMER. Thanks to her multi-disciplinarily and her diverse research background, Dr Kbaier was awarded in February 2016 by two French lecturer qualifications in two different fields. She is Senior Fellow of the Higher Education Academy and an Engineering Professors' Council (EPC) member. Her research was particularly awarded by several productivity bonuses and two IEEE and Spring best paper awards Her research interests include signal processing applied to telecommunications and oceanography, channel coding, digital communications and information theory, error correction in VANET environments, etc.

Carsten Maple Professor Carsten Maple leads the Secure Cyber Systems Research Group in WMG at the University of Warwick, where he is also the Principal Investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research. He is a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity where he leads on Transport Mobility and Warwick PI on the Autotrust project. Carsten has an international research reputation and extensive experience of institutional strategy development and interacting with external agencies. He has published over 250 peer-reviewed papers and is co-author of the UK Security Breach Investigations Report 2010, supported by the Serious Organised Crime Agency and the Police Central e-crime Unit. Additionally he has advised executive and non-executive directors of public sector organisations and multibillion pound private organisations. Professor Maple is a past Chair of the Council of Professors and Heads of Computing in the UK, a member of the Zenzic Strategic Advisory Board, a member of the IoTSF Executive Steering Board, an executive committee member of the EPSRC RAS Network and a member of the UK Computing Research Committee, the ENISA CarSEC expert group, the Interpol Car Cybercrime Expert group and Europol European Cybercrime Centre.